Kaspersky®
Embedded Systems
Security

Comparaison avec la norme PCI DSS v3.2

La norme PCI DSS 3.2 réglemente de nombreuses exigences en matière de sécurité technique et de paramètres de systèmes utilisant les données de carte de crédit. Les sous-sections 1.4, 2.4a, 5.1, 5.1.1, 5.2, 5.3, 6.2, 10.5.5, 11.5 de la norme PCI DSS v3.2 prévoient la réglementation stricte de la protection antivirus liée aux terminaux fonctionnant avec les données détaillées du titulaire d'une carte. Il est fréquent, même si cela ne constitue pas une règle officielle, que les fonctions de contrôle des périphériques et de contrôle d'applications soient considérées comme relevant également de l'audit du logiciel antivirus de la norme PCI DSS.

1.4

EXIGENCES DE LA NORME PCI DSS :

Installer un pare-feu personnel ou une fonction équivalente sur tout appareil informatique portable capable de se connecter à Internet lorsqu'il n'est pas sur le réseau, et qui est également utilisé pour accéder au CDE. Les configurations du pare-feu (ou équivalent) incluent :

- la définition des paramètres de configuration spécifique ;
- l'exécution active d'un pare-feu personnel (ou fonction équivalente) ;
- l'absence de modification du pare-feu personnel (ou fonction équivalente) par les utilisateurs d'appareils informatiques portables.

PROCÉDURES DE TEST :

1.4.a Examiner les stratégies et les normes de configuration afin de confirmer les points suivants :

- pare-feu personnel ou fonction équivalente requis sur tout appareil informatique portable capable de se connecter à Internet lorsqu'il n'est pas sur le réseau, et qui est également utilisé pour accéder au CDE ;
- définition de paramètres de configuration spécifiques pour le pare-feu personnel (ou fonction équivalente) ;
- configuration du pare-feu personnel (ou fonction équivalente) en vue d'une exécution active ;
- configuration du pare-feu personnel (ou fonction équivalente) pour empêcher toute modification par les utilisateurs des appareils informatiques portables.

1.4.b Inspecter un échantillon des appareils de l'entreprise fin de confirmer les éléments suivants :

- l'installation et la configuration du pare-feu personnel (ou fonction équivalente) selon les paramètres de configuration particuliers de l'organisation ;
- l'exécution active d'un pare-feu personnel (ou fonction équivalente) ;
- l'absence de modification du pare-feu personnel (ou fonction équivalente) par les utilisateurs d'appareils informatiques portables.

DIRECTIVES :

Les appareils informatiques portables qui sont autorisés à se connecter à Internet au-delà du pare-feu de l'entreprise sont les plus exposés aux menaces sur Internet. L'adoption d'un pare-feu (par exemple, pare-feu personnel logiciel ou matériel) contribue à protéger les appareils contre les attaques via Internet qui pourraient exploiter l'appareil en vue d'accéder aux systèmes et aux données de l'entreprise après que l'appareil a été reconnecté au réseau.

L'entreprise détermine les paramètres de configuration spécifiques du pare-feu.

2.4a

EXIGENCES DE LA NORME PCI DSS	Tenir un inventaire des composants du système entrant dans le champ d'application de PCI DSS.
PROCÉDURES DE TEST	**2.4.a** Examiner l'inventaire du système afin de confirmer l'existence d'une liste des composants logiciels et matériels et l'existence d'une description de la fonction/de l'utilisation pour chacun.
DIRECTIVES	La tenue d'une liste à jour de l'ensemble des composants système permettra à l'entreprise de définir avec précision et efficacité la portée de l'environnement pour la mise en œuvre des contrôles PCI DSS. Sans inventaire, certains composants système pourraient être oubliés et exclus par inadvertance des normes de configuration de l'entreprise.

5.1

EXIGENCES DE LA NORME PCI DSS :	Déployer des logiciels antivirus sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs).
PROCÉDURES DE TEST :	Sur un échantillon de composants du système comprenant tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants, vérifier que des logiciels antivirus sont déployés et, le cas échéant, qu'une technologie de protection antivirus est en place.
DIRECTIVES :	Les systèmes normalement sécurisés sont l'objet d'attaques constantes utilisant les codes d'exploitation largement publiés, souvent de type « zero-day » (attaque exploitant des vulnérabilités inconnues jusqu'à présent). En l'absence de solution antivirus régulièrement mise à jour, ces nouvelles formes de logiciel malveillant peuvent attaquer les systèmes et désactiver un réseau ou compromettre les données.

5.1.1

EXIGENCES DE LA NORME PCI DSS :	S'assurer que tous les programmes antivirus sont capables de détecter et d'éliminer tous les types de logiciels malveillants connus, et d'assurer une protection efficace.
PROCÉDURES DE TEST :	Examiner la documentation du fournisseur et les configurations d'antivirus pour vérifier que les programmes d'antivirus détectent tous les types de logiciels malveillants connus, éliminent tous les types de logiciels malveillants connus et protègent contre tous les types de logiciels malveillants connus.
DIRECTIVES :	Il est important de se protéger contre TOUS les types et toutes les formes de programmes malveillants.

5.2

EXIGENCES DE LA NORME PCI DSS :	S'assurer que tous les mécanismes antivirus sont maintenus à jour, effectuent régulièrement des analyses et génèrent des journaux d'audit qui sont conservés selon la condition 10.7 de la norme PCI DSS.
PROCÉDURES DE TEST :	**5.2.a** Examiner les politiques et les procédures pour vérifier que les logiciels antivirus et les définitions d'antivirus sont maintenus à jour. **5.2.b** Examiner les configurations antivirus, y compris l'installation du logiciel maître, pour vérifier que les mécanismes antivirus sont configurés pour effectuer automatiquement les mises à jour et pour effectuer régulièrement des scans. **5.2.c** Examiner un échantillon de composants du système, y compris tous les types de systèmes d'exploitation généralement affectés par des logiciels malveillants, pour vérifier que le logiciel antivirus et les définitions sont à jour et que des scans sont effectués régulièrement. **5.2.d** Examiner les configurations antivirus, y compris l'installation du logiciel maître et un échantillon des composants du système pour vérifier que la production de journaux de logiciel antivirus est activée et les journaux sont conservés conformément à la condition 10.7 de la norme PCI DSS.
DIRECTIVES :	Même les meilleures solutions antivirus sont limitées du point de vue de l'efficacité si elles ne sont pas maintenues à jour avec les dernières mises à jour de sécurité, fichiers de signature ou protection contre les logiciels malveillants. Les journaux d'audit permettent de surveiller l'activité des virus et des logiciels malveillants, ainsi que les réactions contre les logiciels malveillants. Par conséquent, il est impératif que la solution antivirus soit configurée pour générer des journaux d'audit et gérer ces derniers conformément à la condition 10.

5.3

EXIGENCES DE LA NORME PCI DSS :	S'assurer que les mécanismes antivirus fonctionnent de manière active et ne peuvent pas être désactivés ou altérés par les utilisateurs, sauf autorisation spécifique de la direction au cas par cas, sur une base limitée dans le temps.
PROCÉDURES DE TEST :	**5.3.a** Examiner les configurations antivirus, y compris l'installation du logiciel maître et un échantillon des composants du système pour vérifier que le logiciel antivirus fonctionne activement. **5.3.b** Examiner les configurations antivirus, y compris l'installation du logiciel maître et un échantillon des composants du système pour vérifier que le logiciel antivirus ne peut pas être désactivé ou altéré par les utilisateurs. **5.3.c** Interroger le personnel responsable et observer les processus pour vérifier que les logiciels antivirus ne peuvent pas être désactivés ou altérés par les utilisateurs, sauf autorisation spécifique de la direction au cas par cas, sur une base limitée dans le temps.
DIRECTIVES :	Un antivirus qui fonctionne continuellement et qui ne peut pas être altéré offrira une sécurité persistante contre les logiciels malveillants. L'utilisation de contrôles basés sur une politique sur tous les systèmes pour assurer que les protections contre les logiciels malveillants ne puissent pas être altérées ou désactivées aidera à empêcher que les faiblesses du système ne soient exploitées par les logiciels malveillants. Des mesures de sécurité supplémentaires peuvent également être mises en œuvre pour la période pendant laquelle la protection antivirus n'est pas active, par exemple déconnecter le système sans protection d'Internet lorsque la protection antivirus est désactivée, et effectuer un scan complet une fois qu'elle est réactivée.

6.2

EXIGENCES DE LA NORME PCI DSS :

S'assurer que tous les logiciels et les composants du système sont protégés de vulnérabilités connues en installant les correctifs de sécurité applicables fournis par le fournisseur. Installer les correctifs de sécurité critiques dans le mois qui suit leur commercialisation.

Remarque : Les correctifs de sécurité critiques doivent être identifiés selon le processus de classement des risques défini par la condition 6.1.

PROCÉDURES DE TEST :

6.2.a Examiner les politiques et procédures relatives à l'installation des correctifs de sécurité pour vérifier que les processus sont définis pour installer les correctifs de sécurité critiques pertinents fournis par le fournisseur dans le mois qui suit leur publication et installer tous les correctifs de sécurité critiques pertinents fournis par le fournisseur dans un délai acceptable (par exemple, dans les trois mois).

6.2.b Pour un échantillon de composants du système et de logiciels associés, comparer la liste des correctifs de sécurité installés sur chaque système avec la liste des correctifs de sécurité les plus récents du fournisseur, pour vérifier que les correctifs de sécurité critiques pertinents fournis par le fournisseur sont installés dans le mois qui suit leur publication et que tous les correctifs de sécurité critiques pertinents fournis par le fournisseur sont installés dans un délai acceptable (par exemple, dans les trois mois).

DIRECTIVES :

Les systèmes normalement sécurisés sont l'objet d'attaques constantes utilisant les codes d'exploitation largement publiés, souvent de type « zero-day » (attaque exploitant des vulnérabilités inconnues jusqu'à présent). Si les correctifs les plus récents ne sont pas appliqués le plus tôt possible sur les systèmes critiques, un individu malveillant peut utiliser des failles pour attaquer ou désactiver al:\Delivery (A-L)\KSP\KSP_HHOATM_014\181 Various ENT_FRENCH\02_Prep\DTP\02_Work\01_for_translation\KL_KESS_PCI_DSS_Doc_3.2_EN\KL_KESS_PCI_DSS_Doc_3.2_EN.inddsystem, ou accéder aux données sensibles.

Établir une priorité des correctifs pour l'infrastructure critique garantit que les systèmes et les dispositifs de haute priorité sont protégés des vulnérabilités aussi tôt que possible après la commercialisation d'un correctif. Envisager de donner la priorité à l'installation de correctifs, de sorte que les correctifs de sécurité pour les systèmes critiques ou à risque soient installés dans les 30 jours et les correctifs de sécurité moins critiques dans les 2-3 mois.

Cette condition s'applique à tous les correctifs applicables pour tous les logiciels installés.

10.5.5

EXIGENCES DE LA NORME PCI DSS :

Utiliser un logiciel de surveillance de l'intégrité des fichiers ou de détection des modifications dans les journaux pour confirmer que les données existantes dans les journaux ne peuvent pas être modifiées sans déclencher des alertes (les nouvelles données ajoutées ne doivent toutefois pas déclencher une alerte).

PROCÉDURES DE TEST :

Examiner les paramètres du système, les fichiers surveillés et les résultats des activités de surveillance afin de vérifier l'utilisation d'un logiciel de surveillance de l'intégrité des fichiers ou de détection des modifications dans les journaux.

DIRECTIVES :

Systèmes de surveillance de l'intégrité des fichiers ou de détection des modifications pour les modifications introduites dans les fichiers critiques et notifications en cas de détection de telles modifications. Dans le cadre de la surveillance de l'intégrité des fichiers, une entité surveille en général les fichiers qui ne sont pas modifiés régulièrement, mais dont la modification signale une compromission éventuelle.

11.5

EXIGENCES DE LA NORME PCI DSS :

Déployer un mécanisme de détection des modifications (par exemple, des outils de surveillance de l'intégrité des fichiers) pour alerter le personnel en cas de modification non autorisée (modifications, ajouts, suppressions) des fichiers système critiques, des fichiers de configuration ou des fichiers de contenu ; configurer le logiciel afin qu'il réalise des comparaisons critiques des fichiers au moins une fois par semaine.

PROCÉDURES DE TEST :

Vérifier l'utilisation d'un mécanisme de détection des modifications en observant les paramètres système et les fichiers surveillés ainsi qu'en consultant les résultats des activités de surveillance.

Exemples de fichiers à surveiller :

- Fichiers exécutables du système
- Fichiers exécutables des applications
- Fichiers de configuration et de paramètres
- Journaux et fichiers d'audit stockés de façon centralisée, historiques ou archivés
- Fichiers critiques complémentaires déterminés par entité (par exemple, via l'évaluation du risque ou d'autres méthodes).

DIRECTIVES :

Solutions de détection des modifications telles que les outils de surveillance de l'intégrité des fichiers pour vérifier les modifications, les ajouts et les suppressions dans les fichiers critiques et envoyer des alertes quand de telles modifications sont détectées. En cas de mise en œuvre inadéquate ou si les résultats de la solution de détection des modifications ne sont pas correctement suivis, un individu malveillant pourrait ajouter, supprimer ou modifier le contenu du fichier de configuration, des applications du système d'exploitation ou des fichiers exécutables d'application. Des modifications non autorisées qui n'ont pas été détectées pourraient rendre inefficaces les contrôles de sécurité et/ou entraîner le vol des données du titulaire de la carte sans impact notable sur le traitement normal.